Architectural Risk Analysis - Business Case

Steven Lavenhar, Cigital, Inc. [vita[1]]
Gary McGraw, Cigital, Inc. [vita[2]]

2005-11-04

Risk analysis is an essential part of the software development life cycle. Performing risk analysis early in the life cycle enhances resource allocation decisions, enables us to compare alternative software architectural designs, and helps in identifying high-risk components in the system. As a result, remedial actions to control and optimize the process and improve the quality of the software product can be taken.

Risk is part of any capital investment. Identifying and controlling architectural risks can have a significant impact on the overall success of a software development project. However, risk is not the only consideration for investment evaluations. Investments with high technical risk may be selected if the investment is deemed a strategic or operational necessity. Other investments may be selected simply because they have low risk and require few resources. Conducting a risk analysis and controlling risk is a continuing process throughout the investment/development life cycle.

Architectural risks can be viewed in terms of threats, vulnerabilities, and costs. In organizations already performing architectural risk analyses, there is already an awareness of their risk profile, threats, ease of exploitation, impact, and risk exposure levels. Such organizations are aware of levels of "acceptable" risk and are cognizant of what risks their organizations are willing to accept. Strategic planning by these companies allows them to review the risk mitigation strategies and consider the costs associated with the original cost of the risk, as compared to the cost of risk mitigation.

In addition to prioritized risks, a primary output of the architectural risk analysis is an overall “risk factor” that can be applied to each risk. The risk factor is calculated by determining the impact a particular risk will have on the investment if it is realized and the likelihood of this risk occurring. Calculating the risk factor for each identified investment risk and summing the risk factors will determine an overall risk rating for the investment. This overall risk rating should reflect the risk-adjusted ROI for the investment.

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/197-BSI.html (Lavenhar, Steven)
2. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/198-BSI.html (McGraw, Gary)
1. mailto:copyright@cigital.com